DAS Information Security Office
Monthly Security Tips
NEWSLETTER

July 2008 Volume 3, Issue 6

Data Breach

From the DAS Information Security Office

What is a Data Breach?

Data breach generally refers to instances where personal information is lost, stolen, hacked into, or accessed without permission. Organizations and individuals have the responsibility of protecting confidential or sensitive information in their care and proper safekeeping of this data is vital. Failure to do so can result not only in a breach, but also lead to damaged reputation, significant fines or loss of revenue, and other negative consequences.

Data breaches occur all too frequently, in both large and small organizations. The public and private sectors have been affected by data breaches. The scope of this issue is large with more than 227 million records nationwide involved in a breach since February 2005. This figure represents only those breaches that have been reported, so it may reflect only a portion of the actual occurrences. This is an issue that everyone must be aware of and take steps to mitigate.

In addition to data breach concerns, we must also recognize that data manipulation is a potential threat. If we cannot trust the integrity of our data, and know that it has not been altered inappropriately, our ability to carry out our mission and serve our customers becomes impaired.

Some examples of data that must be protected include the following:

- Customer/employee information such as names, Social Security numbers, credit card numbers;
- Passwords and other computer security-related information;
- Intellectual property;
- Financial information; and
- Health records of individuals.

How is Data Compromised or Disclosed?

Hacking is one method of obtaining data such as Social Security numbers and credit card accounts. Attackers may also use social engineering, phishing or other similar attempts to gain access. These activities can translate into very large sums of revenue for those in the organized crime world. While very sophisticated techniques are sometimes used to steal sensitive data, one of the most common threats comes from within the organization itself. According to Deloitte's *2007 Global Security Survey*, 65 percent of respondents reported repeated external breaches. Of those incidents, 18 percent stemmed from unintentional data leakage. The report also indicates that some of the surveyed data breaches went undetected for extended periods.

The loss or theft of data is not limited to electronic data loss or computer hacking. Other possibilities include theft or loss of laptops, tapes and flash-drive devices or improper disposal of hard copy documents and computer equipment.

Are there Laws or Regulations to Protect Data?

There are laws and regulations to regulate how organizations must handle and protect sensitive information. Some of the most notable include the following:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- Payment Card Industry (PCI) Data Security Standard; and
- Family Educational Rights and Privacy Act (FERPA).

There are Breach Notification Laws currently in place in forty-two states and the District of Columbia which govern the notification of an individual whose personal information has, or may have been disclosed.

The State of Iowa recently enacted a data breach notification law which went into effect July 1, 2008. The law requires that organizations with a data breach involving personal information notify individuals affected by the breach. The notification provision (set out in Senate File 2308) requires that notices include:

- A description of the breach;
- The date of the breach;
- The type of personal information disclosed in the breach;
- Contact information for consumer reporting agencies; and
- Advice for reporting identity theft.

What Can I Do?

Organizations and individuals must take proactive measures to minimize the risk of data breach. Everyone in an organization has a role in protecting information. The following are examples of steps you can take to help prevent data disclosure:

- Follow your organization's cyber/information security policies;
- Know how your organization has classified information and adhere to the appropriate controls in place;
- Follow proper procedures for the destruction or disposal of media that contain sensitive data;
- Participate in security awareness training.

Remember, cyber security is everyone's responsibility. Don't be the weak link in the chain.

For more cyber security monthly tips go to: www.msisac.org/awareness/news/

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture.

Brought to you by:

MS-ISAC

www.msisac.org